Informe

Investigación sobre seguridad digital con organizaciones sociales de Chiapas



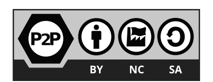
Comunicación
Cultura Digital

Informe

Investigación sobre seguridad digital con organizaciones sociales de Chiapas

AGRADECIMIENTOS:
A las organizaciones que participaron en esta investigación, a Access Now por el apoyo para realizar este proyecto, y a todas las personas que han aportado para el desarrollo de este informe.

CRÉDITOS:
Coordinación: Sursiendo
Textos y edición: la_jes y dom
Revisión: Paola Ricaurte
Diseño editorial: Irene Soria
Traducción al inglés: Nàdege.
Imágenes: la_jes



Índice

0. Presentación



Este es el informe sobre uno de los caminos recorridos durante 2018 como Sursiendo, donde hemos convivido con lo local y lo digital, en un proyecto-proceso de investigación con organizaciones sociales de Chiapas para realizar un diagnóstico sobre seguridad digital.

Estar en línea es muy importante para gran parte de la población. También para el trabajo de defensa de derechos humanos

Según un estudio de Lori Lewis y Chadd Callahan (Desjardins, 2018), con datos de mayo de 2018, en una hora se envían más de 10.000 millones de emails, se descargan 22 millones de aplicaciones o se realizan 222 millones de consultas en buscadores. En México, más del 65% de la población está conectada, según datos de Internet World Stats (2018).

Hoy en día Internet es fundamental para entender cómo funcionan nuestras sociedades, ya que está presente en casi todos los ámbitos sociales, políticos, económicos y culturales de México y del mundo. Estar en línea es muy importante para gran parte de la población. También para el trabajo de defensa de derechos humanos.

Más allá de las cifras pensamos que debemos fijarnos más en los quiénes, los cómos y los qués. Cómo usamos y nos relacionamos a través de Internet, y a través de qué dispositivos y programas. Qué ponemos en riesgo al estar en línea.

Nos gusta pensar Internet como un territorio, "como el espacio vivido, sentido y parte integrante de su cotidianidad", según lo define Arturo Escobar (2010); el territorio es el escenario de las relaciones sociales, por eso vemos Internet como una



Pero ese territorio, como muchos otros, está amenazado por el neoliberalismo, a través de la vigilancia y el control, la criminalización y el despojo, la comercialización de datos personales y la falta de ética

construcción social y nuestro conocimiento del mismo implica el conocimiento del proceso de su producción, de su 'habitarlo'. Pero ese territorio, como muchos otros, está amenazado por el neoliberalismo, a través de la vigilancia y el control, la criminalización y el despojo, la comercialización de datos personales y la falta de ética. Internet es un territorio en disputa.

Así, durante todo el año 2018 nos propusimos realizar una investigación sobre una parte de esta disputa: la seguridad digital en organizaciones sociales de Chiapas, con el fin de realizar un diagnóstico de la situación de este tema en la región.

En México, la situación de la seguridad digital atraviesa momentos de amenaza a organizaciones, activistas sociales y defensoras de derechos humanos, como hemos visto con el despliegue de la vigilancia de Estado y los casos de utilización de *software* de espionaje Galileo, de la empresa Hacking Team, o Pegasus, de NSO Group, además de criminalización y censura. Tanto instituciones públicas como corporaciones tecnológicas ponen en riesgo la seguridad en el trabajo de defensoría y acompañamiento a procesos colectivos, que también se ve afectada por el crimen organizado.

Internet es un territorio en disputa

Nos planteamos hacer un proceso de diagnóstico basado en metodologías de la educación popular y dinámicas participativas con talleres, encuestas, entrevistas y fichas de información en la red, yendo a sus contextos, conociendo sus espacios; para pasar a analizar toda esa información y posteriormente hacer una devolución que sirviese

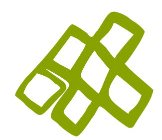
para mejorar las prácticas que se tienen en los entornos digitales, y así tener una base firme para realizar un acompañamiento de largo plazo.

Pero ¿qué es la seguridad digital? En algunos casos es definida como la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras; o también se puede definir como las prácticas y las herramientas que utilizamos las y los usuarios para proteger aparatos, información e interacciones digitales.

Mucho de eso hay, pero desde Sursiendo preferimos ver la 'seguridad digital' como las prácticas de autodefensa y autocuidados digitales, como las formas de mejorar nuestra 'vida digital' en un (largo) camino hacia la soberanía tecnológica. O como también describen algunas de las personas de las organizaciones participantes: "una serie de hábitos, herramientas que uno utiliza en su cotidiano para poder proteger la información" o "la posibilidad de moverme por el ciberespacio sin que eso me pusiera en un riesgo no elegido. Ni a mí, ni a las personas que me rodean, ni en el trabajo".

Consideramos que la 'seguridad' como concepto es en sí mismo engañoso y ha desembocado en el estado de vigilancia en el que cual estamos actualmente. No hay manera posible de estar 'seguras y seguros' al 100%, pero sí podemos tomar medidas para cuidar nuestras acciones digitales y así cuidar también nuestro trabajo de defensoría y activismos.

Desde Sursiendo, preferimos ver la 'seguridad digital' como las prácticas de autodefensa y autocuidados digitales, como las formas de mejorar nuestra 'vida digital' en un largo camino hacia la soberanía tecnológica









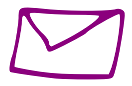
En las siguientes páginas hacemos un resumen de qué ha pasado con la seguridad digital en México y en Chiapas, cuáles han sido los hallazgos de la investigación y qué necesidades y retos se plantean

Sin embargo, y debido a que el concepto de 'seguridad digital' ha adquirido una utilización más generalizada para hablar de este tema, lo nombraremos de este modo a lo largo de todo el informe.

Este proceso de diagnóstico ha sido realizado con ocho organizaciones de Chiapas que trabajan distintos ámbitos, como los derechos humanos, migraciones, derechos de las mujeres, defensa de la tierra y el territorio, acompañamiento a comunidades en resistencia o con propuestas alternativas al modelo extractivo de "desarrollo". Por guardar la confidencialidad y proteger sus procesos no se mencionan sus nombres en este informe.

En las siguientes páginas hacemos un resumen de qué ha pasado con la seguridad digital en México y en Chiapas, cuáles han sido los hallazgos de la investigación y qué necesidades y retos se plantean.

Queremos agradecer a las organizaciones su participación y confianza en este camino, que aún continua. Al Centro de Derechos Humanos Fray Bartolomé de Las Casas (Frayba), por compartirnos su experiencia y a Paola Ricaurte por sus aportaciones a este informe.





1. Contexto de vigilancia



El sociólogo e investigador David Lyon define la vigilancia como “la atención dirigida, sistemática y cotidiana a detalles personales por motivos de influencia, manejo, protección o dirección” (Bauman y Lyon, 2013).

Pero en la era digital la vigilancia no solo es cotidiana sino también ubicua: es una recolección de información que ya no necesariamente es dirigida y enfocada, sino masiva y generalizada, implementada tanto por Estados como por corporaciones, mayormente con sede en Estados Unidos y Europa.

La directora de una de las organizaciones comenta: "yo creo que para quienes quieran tener tus datos es muy fácil tenerlos"; u otra persona participante también expresa: "decir ‘no tengo nada que esconder’ es muy fácil, pero todos tenemos cosas que no queremos que estén ahí".

Además, toda la información recopilada de las redes digitales suele ser almacenada en varias copias y por un tiempo indefinido. La captura, almacenaje y análisis es un proceso automatizado que no requiere grandes esfuerzos (aunque sí recursos), por lo que resulta más simple capturarlo y guardarlo todo en caso de que alguna vez fuera de utilidad. Por otra parte, las plataformas de las corporaciones usadas habitualmente no presentan información transparente sobre el uso de los datos que guardan y hacer un verdadero control sobre ellas no siempre es posible.

Las plataformas de las corporaciones usadas habitualmente no presentan información transparente sobre el uso de los datos que guardan y hacer un verdadero control sobre ellas no siempre es posible

"En resumen, la vigilancia de la comunicación digital es ubicua, automática, efectiva y vive para siempre. Se podrá seguramente encriptar la comunicación pero su patrón de comunicación y las relaciones serán difíciles de proteger de la exposición" (Sparrow, 2014).

1.1 Brevísima historia de la vigilancia digital en México

Son representativas las palabras de Jorge Hernández, del Frayba, cuando nos explica en la entrevista que:

"el primer desafío como defensores de derechos humanos es que tenemos que saber exactamente dónde estamos parados, no podemos ser un o una defensora de derechos humanos 'inocente', no podemos dejar de conocer el contexto, los intereses que estamos tocando; el segundo, es que si bien el Estado es el primer responsable de la protección del trabajo de derechos humanos, la seguridad tiene que ser mía y de mi colectivo, sin quitarle el dedo al Estado. Tenemos que tomar en cuenta que vivimos en un Estado opresor, un Estado espía, un Estado que utiliza el control, el miedo y la represión como un método de control de la población".

En México han habido varios casos de vigilancia y criminalización a través de Internet, compra de *software* espía y uso de éste contra activistas, periodistas, defensores y defensoras de derechos humanos, que han sido documentados y analizados por organismos sociales; casos que recoge-

En México han habido varios casos de vigilancia y criminalización a través de Internet, compra de software espía y uso de éste contra activistas, periodistas, defensores y defensoras de derechos humanos



mos aquí basándonos en noticias e informes publicados.

La Constitución Política de los Estados Unidos Mexicanos reconoce el respeto a los derechos humanos. Entre ellos establece la protección del derecho a la privacidad en cuanto a la información que se refiere a la vida privada (de su persona, familia, residencia, documentos o posesiones) (Laurant y Laguna Osorio, 2014).

El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) es la institución encargada de salvaguardar los derechos individuales a la protección de datos, mientras que la única ley federal que rige la privacidad y protección de datos en posesión de particulares es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que el Congreso de la Unión promulgó en julio de 2010. Su ámbito de aplicación incluye a los individuos y las empresas, no a gobiernos ni otras entidades públicas (Laurant y Laguna Osorio, 2014). Por otro lado, la Suprema Corte también ha dictaminado que las comunicaciones privadas están protegidas constitucionalmente de vigilancia en tiempo real, así como de interferencia en el **hardware** donde se almacenan.

En resumen, la prohibición del espionaje es explícita en la Constitución, y también existe un marco jurídico para la protección de datos personales respecto a particulares, pero en cuanto al espionaje gubernamental el marco legal es laxo (Rodríguez García, 2017).

La prohibición del espionaje es explícita en la Constitución, y también existe un marco jurídico para la protección de datos personales respecto a particulares, pero en cuanto al espionaje gubernamental el marco legal es laxo









Por otro lado, en México no existe regulación específica sobre herramientas altamente intrusivas de vigilancia como el uso de *software* espía. No obstante, la legislación reconoce la posibilidad de que algunas autoridades puedan requerir autorización judicial federal para la intervención de comunicaciones privadas para fines específicos (R3D, 2017).

En 2009, la Ley Federal de Telecomunicaciones fue modificada para que los proveedores de servicios de telecomunicaciones guardaran el tráfico de datos de comunicación (metadatos) incluyendo el tipo de comunicación, los servicios utilizados, el origen y el destino de las comunicaciones, fecha, hora y duración de las comunicaciones y hasta la localización geográfica de los dispositivos de comunicación por un periodo de al menos doce meses.

En 2012, la Ley Federal de Telecomunicaciones fue nuevamente modificada estableciendo que las empresas de telecomunicaciones tienen la obligación de cooperar con la Fiscalía General y la Fiscalía Estatal para proveer la localización geográfica en tiempo real de dispositivos celulares de comunicación sin la necesidad de una orden judicial.

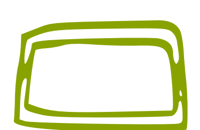
En 2013 se realizó una nueva reforma a la Ley de Telecomunicaciones (publicada finalmente en 2014), que incluye la ampliación de métodos de vigilancia en las comunicaciones. Se incrementa la retención de datos a un periodo de 24 meses y permite que sean almacenados por tiempo indefi-

nido con la sola solicitud de una autoridad de gobierno. También permite que autoridades fuera del sistema penal, como el CISEN, el Ejército, la Armada, y la Policía Federal, puedan determinar la localización geográfica de los dispositivos de comunicación móvil en tiempo real y acceder a los datos guardados por las compañías de telecomunicaciones sin tener que asegurar una orden judicial, bajo la vaga y ambigua premisa de combatir delitos graves (LFTR, 2014).

El Ejército podrá exigirle a nuestro proveedor de acceso a Internet el registro de nuestras comunicaciones

En los últimos años, las leyes, regulaciones y el presupuesto nacional destinado a vigilancia han sufrido cambios drásticos. Sobre el trasfondo de la mal llamada "guerra contra el narco", e impulsado por acuerdos de cooperación internacional sobre seguridad como la "Iniciativa Mérida", México ha experimentado una serie de reformas legales que permiten un incremento en los poderes y técnicas de vigilancia disponibles para las agencias de seguridad, ya sea para la investigación y procesamiento de crímenes o para la prevención de "amenazas a la seguridad nacional".

Para la organización internacional Artículo 19, estas medidas son contrarias a los derechos humanos porque dan pie a una "vigilancia masiva". "[se da] la capacidad de recolectar todos los datos que nuestras comunicaciones y actividad en línea generen sin control judicial. Es decir, el Ejército podrá exigirle a nuestro proveedor de acceso a Internet el registro de nuestras comunicaciones. Además, se tendrá una plataforma que monitoree en tiempo real cada paso que damos, dónde estamos, con quién nos reunimos y cualquier huella di-



Está claro que las técnicas y poderes de espionaje no están siendo utilizados para prevenir "amenazas a la seguridad nacional" o para detener crímenes, o al narcotráfico

gital que generemos", señaló esta organización (CNNMéxico, 2014).

El 99% de la utilización de actos de vigilancia a las comunicaciones se hacen de manera ilegal, según un informe de la Red en Defensa de los Derechos Digitales (Pérez de Acha, 2016; R3D, 2016). La laxitud del Estado mexicano frente a la práctica de espionaje para darle un uso político no ha variado ni siquiera con los numerosos casos registrados al convertirse en escándalo a partir de filtraciones a la prensa en diferentes coyunturas.

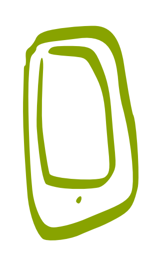
Está claro que las técnicas y poderes de espionaje no están siendo utilizados para prevenir "amenazas a la seguridad nacional" o para detener crímenes, o al narcotráfico. La mayoría de las veces son utilizados contra aquellas personas que cuestionan las prácticas del poder actual, defensores de derechos humanos, periodistas, activistas, etc. En los últimos años se ha destapado una serie de casos de programas utilizados por el gobierno de México para espiar a dichos actores, ya que una parte medular de la estrategia ha sido mantener 'mano de hierro' sobre los medios de comunicación y silenciar las voces críticas, incluyendo aquellas de la Internet, y así limitar la libertad de expresión.

1.2. Gobierno, empresas y spyware

Desde 2007 se han publicado reportes sobre la cooperación del gobierno mexicano con el de Estados Unidos para intervenir llamadas telefónicas y correos electrónicos con el equipo de la compañía Verint.



En 2012 se hizo público que el Departamento de Defensa Nacional tenía contratos para adquirir tecnología de vigilancia y equipo con capacidad para monitorear correos, interferencia de voz, ruido de fondo, captura de imágenes, extracción de SMS y MMS, listas de contactos, registros de calendarios, localización GPS y capturas de pantallas, acceso y manipulación de los documentos del sistema, información de la tarjeta SIM, información de hardware, etc.



Un año después, la organización canadiense Citizen Lab reveló que el software de espionaje Finfisher, de la empresa inglesa Gamma International, y Da Vinci, de la empresa italiana Hacking Team, fueron usados para espiar a defensores de derechos humanos, activistas y periodistas (Flores, 2015). Por ese entonces, salieron a la luz informaciones sobre que las empresas Gamma Group y Hacking Team enviaron en 2013 a México a miembros de sus equipos, según información proporcionada por Wikileaks a La Jornada (Miguel y Molina, 2013). Ese mismo año, algunos medios se hicieron eco de los contratos de la Procuraduría General para adquirir software espía en 2012 (Reforma, 2013).

En 2012 se hizo público que el Departamento de Defensa Nacional tenía contratos para adquirir tecnología de vigilancia y equipo con capacidad para monitorear correos

Entre 2014 y 2016 siguieron saliendo informaciones sobre el software espía en diversos medios, donde expresaban que "México es el país que más gastó en Hacking Team para espiar a sus ciudadanos" (Lacort, 2015), detallando qué instituciones y Estados de la República y cuánto dinero habían invertido.

"Hay un registro impresionante de nuestra vida, inclusive de nuestros aspectos que podrían ser privados, íntimos, familiares están registrados por todos los medios digitales posibles"

En 2017 se lanzó la campaña #GobiernoEspía, en la que organizaciones mexicanas, con el apoyo de Citizen Lab y algunos medios de comunicación (como The New York Times) (Ahmed y Perlroth, 2017), daban muestras de que instancias de Gobierno Federal de México y algunos estados habían adquirido y utilizado el *spyware* Pegasus, de la empresa israelí NSO Group, usado una vez más para vigilar a periodistas, defensores y defensoras de derechos humanos y activistas, violando gravemente sus derechos.

La instalación de este sofisticado *software* espía permite al atacante tomar control de diferentes funciones del teléfono y acceder a los contenidos del aparato permitiendo monitorear cualquier detalle de la vida diaria de una persona por medio de su celular. A pesar de las denuncias, en septiembre de 2018 Citizen Lab confirmó que el *software* Pegasus aún continua activo en México.

"Hay un registro impresionante de nuestra vida, inclusive de nuestros aspectos que podrían ser privados, íntimos, familiares están registrados por todos los medios digitales posibles", reflexionaba el encargado de comunicación de una de las organizaciones participantes de la investigación.

1.3 La situación de la vigilancia en Chiapas

En 2010, Héctor Bautista, miembro de la comunidad de *software* libre y administrador de la página web InfoChiapas.com, fue arrestado por la policía estatal por cargos de pornografía infantil. Fue confiscada su computadora y sus tarjetas de memoria.



Según parece, realmente fue arrestado por la publicación de un artículo que hablaba de la deuda del gobierno. Estuvo 40 días en custodia y después fue liberado (SIPAZ, 2010).

Tres años después, en 2013, fue detenido Gustavo Maldonado (Mariscal, 2013), acusado de narcomenudeo bajo un caso lleno de irregularidades. Maldonado fue crítico con el gobierno de Chiapas en redes sociales digitales, y en meses anteriores había llamado a manifestaciones por el tema del agua en Tuxtla, la capital chiapaneca. La tarde de su arresto había publicado un video y retuiteado información sobre la compra de *Blackeyed Hosting Monitors*, equipo de vigilancia para localizar activistas digitales en Chiapas. Maldonado fue liberado después de haber estado 90 días detenido (Robles Maloof, 2013).

Cuando el 8 de julio de 2015, Wikileaks publicó los más de un millón de correos electrónicos filtrados del proveedor italiano de *malware* de vigilancia Hacking Team, el gobierno de Chiapas figuraba entre sus posibles clientes (Wikileaks, 2015). Sin embargo, el inicio de las negociaciones parece haber sido un año antes, como se menciona en un correo de febrero de 2014, a través de un empleado de la consultora mexicana White Hat Consultores, una empresa con "alta especialización en servicios de seguridad de la información y ciberseguridad, con especial presencia en los mercados de gobierno, financiero y de servicios". Para junio de 2015, un empleado de otra empresa mexicana, Heres, aseguraba haber conversado con dos dependencias del gobierno chiapaneco del

La tarde de su arresto, Gustavo Maldonado, había publicado un video y retuiteado información sobre la compra de Blackeyed Hosting Monitors, un equipo de vigilancia para localizar activistas digitales en Chiapas

En los últimos 10 años las intervenciones telefónicas tanto de teléfonos personales de las y los defensores de derechos humanos como los organizacionales, la criminalización, hostigamiento y persecuciones físicas han aumentado considerablemente

área de seguridad que estaban "interesadas en conocer la propuesta de Hacking Team".

El contexto general de violencia y persecución en Chiapas se ha visto incrementado en los últimos años. Y de formas que antes no eran imaginables. En una de las entrevistas de nuestra investigación, una defensora con muchos años de experiencia en el Estado, nos relataba sorprendida: "Sí, [la vigilancia] está súper alucinante en el momento, cosas de ciencia ficción. Big brother is watching you todo el mundo lo sabía. Pero estás descubriendo cosas que ni pensabas que eran posibles. Ni tecnológicamente ni mucho menos éticamente". Del mismo modo, en otra de las entrevistas se hacía mención a que durante las acciones contra las Reformas Estructurales grupos que trabajan en seguridad del Estado "ponían un carro y ahí captaban un montón de cosas, de repente hay una palabra que se repite muchísimas veces entonces sobre eso ven quien, de dónde está saliendo y entonces eso es lo que siguen".

Además, en los últimos 10 años las intervenciones telefónicas tanto de teléfonos personales de las y los defensores de derechos humanos como los organizacionales, la criminalización, hostigamiento y persecuciones físicas han aumentado considerablemente. Aunque, como nos comentaban, "últimamente veo que no es necesario que se asomen físicamente; si dejan que los veas es solo para que sepas que te están viendo. Pero hoy en día obviamente todo el tema de la vigilancia está en los teléfonos, en tus cuentas de correo, en el dron que puede estar sobre tu casa y tú ni en

cuenta, en la localización satelital, en las cámaras si vas para Tuxtla o Chamula. Entonces hay un registro impresionante de nuestra vida, incluso de nuestros aspectos que podrían ser privados, íntimos, familiares están registrados por todos los medios digitales posibles".

Metadatos

Los metadatos de comunicaciones son datos sobre las comunicaciones de una persona, por ejemplo: los números telefónicos de origen y destino de una comunicación; la hora, fecha y duración de la misma; los datos de identificación de la tarjeta SIM (IMSI) y del dispositivo (IMEI); e incluso los datos de localización de las antenas a las cuáles se conecta un dispositivo móvil.

De manera frecuente se pretende minimizar cuán invasiva puede ser la recolección, almacenamiento y análisis de metadatos de comunicaciones, en particular respecto del contenido de las comunicaciones. Sin embargo, los metadatos de comunicaciones pueden revelar tanta o mucha más información personal que el contenido mismo de las comunicaciones.

Recogido de: Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control. https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf



2. La investigación



2.1 El inicio, las metodologías y el análisis de datos del diagnóstico

Para la presente investigación trabajamos con ocho organizaciones sociales del Estado de Chiapas. La selección de las organizaciones respondió, por un lado, al conocimiento previo que tenemos sobre la labor desarrollada por dichas organizaciones, y por otro, a las diferentes áreas de la defensa de los derechos humanos en la que cada una de ellas se desenvuelve.

Trabajamos con organizaciones defensoras de derechos humanos, defensa de la tierra y el territorio, derechos de las mujeres, derechos de las personas migrantes y derecho a la educación, asentadas en diversas geografías del Estado.

Para sumar a la investigación quisimos también conocer la opinión del Centro de Derechos Humanos Fray Bartolomé de Las Casas (Frayba), quienes desde hace alrededor de ocho años iniciaron un proceso para mejorar su seguridad digital. Jorge Hernández, integrante de la organización, nos comentaba que el Frayba considera la seguridad integral como una tema de apuesta política porque según sus análisis "no hay defensores de derechos humanos de bajo perfil, todos tocamos intereses que al Estado no le gusta que le toquen, señalamos ciertas cosas que al Estado no le gustaría que salieran públicas" y en ese sentido todas las personas defensoras están en riesgo.

A lo largo del proceso de diagnóstico se trabajó con metodologías participativas y se utilizaron

"No hay defensores de derechos humanos de bajo perfil, todos tocamos intereses que al Estado no le gusta que le toquen, señalamos ciertas cosas que al Estado no le gustaría que salieran públicas"

cinco diferentes técnicas de investigación para poder realizar un análisis a profundidad que nos permitiera establecer una suerte de 'línea base' en relación al estado actual de la seguridad digital en organizaciones de Chiapas.

El principal objetivo de la presente investigación radicaba en conocer las necesidades particulares de cada una de las organizaciones participantes para poder adecuar mecanismos que propicien una apropiación de prácticas y herramientas de seguridad digital en el ejercicio de sus acciones de defensoría ya que, como fue mencionando en varias oportunidades, si bien el Estado mexicano tiene la obligación de garantizar la labor de las y los defensores de derechos humanos, no es posible confiar en que ello sucederá y es por eso que las personas defensoras asumen como propias las prácticas más básicas de sus cuidados y autocuidados.



El diagnóstico contó con cinco fuentes de información:

- una ficha con investigación previa, conteniendo la información pública disponible sobre cada una de las organizaciones y las personas más visibles dentro de ellas, en total 8;
- talleres presenciales de diagnóstico con las personas miembros de las organizaciones, en total 8;
- notas de campo tomadas durante los talleres;
- una encuesta completada por las personas integrantes de las organizaciones con información básica sobre uso de medios digitales, dispositivos, sistemas operativos, percepción de su seguridad organizacional, etc; en total 71;
- entrevistas a profundidad realizadas a algunas personas miembros de cada una de las organizaciones con las que trabajamos; en total 16.

En cuanto a la propia metodología, nos inspiramos fundamentalmente en tres herramientas participativas:

- investigación-acción participativa (IAP) (Wikipedia, s/f), cuyo enfoque de investigación en comunidades enfatiza la implicación y la actuación. Con ello, se busca entender el mundo intentando cambiarlo, colaborativamente y siguiendo la reflexión;
- informa-acción, herramienta desarrollada por Mining Watch Canada, el Observatorio de Conflictos Mineros de América Latina y el Observatorio Latinoamericano de Conflictos Ambientales que aborda los diferentes actores involucrados en los temas de interés a través del mapeo de datos;
- diagnósticos en seguridad digital para organiza-

En cuanto a la propia metodología, nos inspiramos fundamentalmente en tres herramientas participativas: investigación-acción participativa, informa-acción y diagnósticos en seguridad digital para organizaciones

Nos propusimos como tarea esencial hacer talleres de devolución con las organizaciones sociales, en los que presentáramos individualmente los resultados de la investigación y retribuyéramos la generosidad y confianza con la que se compartieron

ciones de derechos humanos y derechos territoriales: un manual para facilitadores, diseñado por Técnicas Rudas que, abordando un modelo de amenazas clásico, profundiza el conocimiento sobre usos, riesgos y amenazas en el entorno digital para las personas miembros de las organizaciones.

En diversos momentos de la investigación recurrimos a medios analógicos para dar los siguientes pasos. El momento del análisis de los datos fue unos de ellos. Consideramos que en papel "pensamos mejor" y es por ello que quisimos usar "otras" tecnologías para ir sumando las diversas voces recogidas a través de todas las fuentes de información mencionadas con anterioridad.

Nos comentó un participante en los talleres: "en este ejercicio que hicimos con Sursiendo fue súper interesante de ver gráficamente cómo estamos tan conectados. Todo el mundo está ahí y cómo se interconecta todo. Y de lo que hacemos uso todo el rato".

Finalmente mencionar que como parte de esta primera etapa de diagnóstico e investigación, nos propusimos como tarea esencial hacer talleres de devolución con las organizaciones sociales, en los que presentáramos individualmente los resultados de la investigación y retribuyéramos la generosidad y confianza con la que se compartieron. Para quienes participamos en la propuesta de investigación es fundamental acabar con el modelo extractivo actual, incluido también todo aquello relacionado con la información y la investigación

en la que las personas involucradas rara vez se ven beneficiadas. Entonces, en la última parte del año nos dimos a la tarea de hacer reuniones de devolución, donde también llevamos algunos de los aprendizajes a la práctica.

2.2 Algunos hallazgos

"Hasta hemos tenido que quitar los correos personales de la página web de la organización", relataba el coordinador de una de las organizaciones de Chiapas participantes en este proceso de diagnóstico. Es una frase muy significativa, que de fondo muestra en qué se ha convertido Internet para muchos y muchas defensoras de derechos humanos y activistas.



Hemos visto que existe preocupación por la vigilancia que realizan algunas instituciones locales, estatales, nacionales e internacionales, el crimen organizado y empresas extractivistas que operan en la región

Proporcionar datos personales, formas de contacto, ubicación o itinerarios, comentarios sobre la familia, fotos de viajes, información sensible sobre contrapartes, etc. puede ser utilizado por quienes quieren entorpecer la labor de defensoras y defensores. Si a esto sumamos el uso de redes no seguras, de aplicaciones que comercian con nuestros datos, de *software* fácilmente espiado, el robo o la pérdida de dispositivos y demás, entonces la situación de vulnerabilidad resulta mayor.

INFORMACIÓN SENSIBLE A RESGUARDAR

"La mayor parte de información es sensible, es confidencial, y los mecanismos que usamos son poco seguros o vulnerables", nos decía en entrevista el coordinador de una de las organizaciones. Además, resaltaba, como otras personas participantes, que la información más importante es la de las personas y procesos que acompañan, sumado a los datos personales y familiares.

En líneas generales hemos visto que existe preocupación por la vigilancia que realizan algunas instituciones (locales, estatales, nacionales e internacionales), el crimen organizado y empresas extractivistas que operan en la región (mineras, hidroeléctricas, etc). Sobre todo en la obtención de datos de ubicación, familiares y personales que pongan en riesgo la vida de las personas que trabajan en las organizaciones, de las personas con las que colaboran y del entorno cercano; también hay temor a la pérdida del control de los datos referidos a la gestión interna, repositorio de documentos organizativos o reuniones estratégicas

para el funcionamiento de defensoría, acompañamiento o proyectos.

"Sé que todo está controlado por el Estado, que alguien más puede utilizar tus datos personales, lo que subes, el robo de identidad y muchas cosas. Por esto siempre ha sido el tener cuidado de no subir cosas, de tener resguardada cosas, tratar de prevenir (...) o que la misma información sirva para ponerme en riesgo a mí y a quienes están a mi alrededor", nos dijo una defensora de derechos de la mujer participante en el diagnóstico.

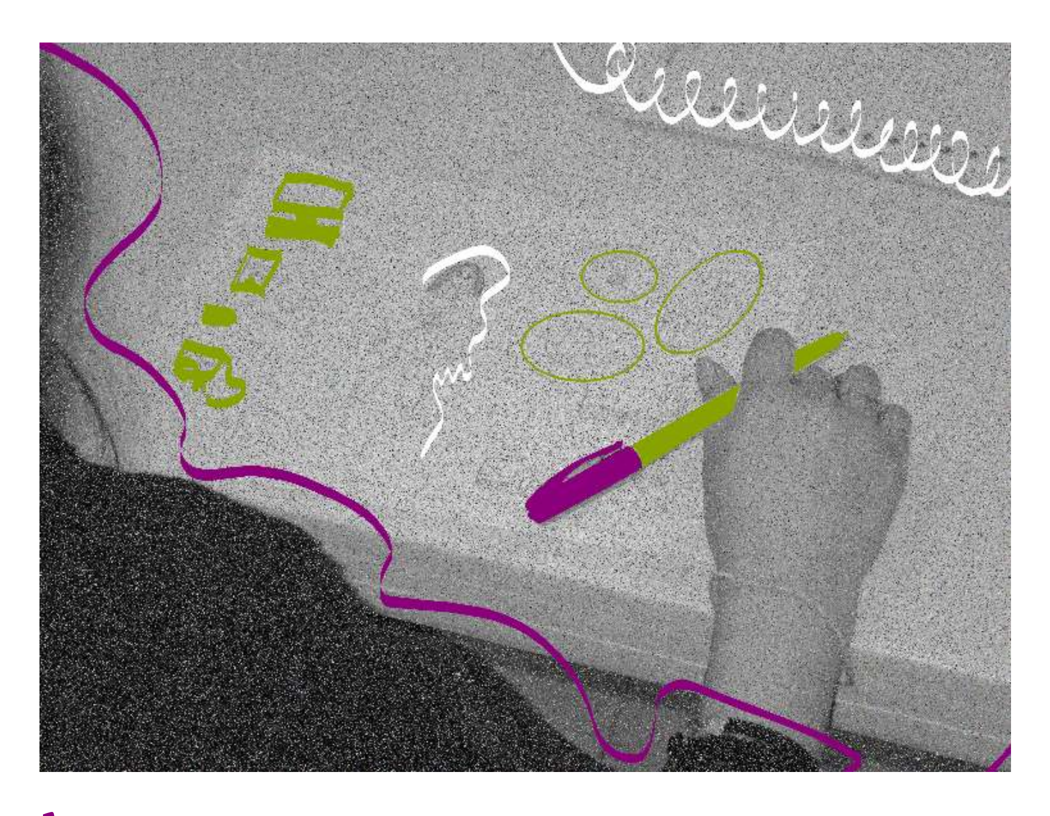
En concreto, se presenta la coincidencia de preocupación en que se vulnere la privacidad de las comunicaciones, pero sobre todo en momentos de articulación en línea o monitoreo de actividades. Por ejemplo, hay inquietud en no poder realizar videollamadas con tranquilidad, temiendo que estén siendo interceptadas o recopilando lo que se mencione; o que se pueda acceder al intercambio de mensajes a través de WhatsApp o cualquier otra aplicación parecida, en situaciones cotidianas y, sobre todo, en situaciones de monitoreo de actividades. El uso de correo electrónico, herramienta fundamental en el trabajo de las organizaciones, también entraña riesgos conocidos por las y los defensores, como pueden ser la fuga de información y la entrada de virus o malware.

Se presenta la coincidencia de preocupación en que se vulnere la privacidad de las comunicaciones, pero sobre todo en momentos de articulación en línea o monitoreo de actividades

Las redes sociales (tipo Facebook o Instagram) aparecen como preocupaciones, por esa fuga de información, que hacemos pública o está disponible para la empresa, o como fuente de hostigamiento. Y la navegación y las búsquedas, cuando

se las confiamos a una empresa todopoderosa como Google, a través del navegador Chrome o su buscador.

También existe preocupación en las informaciones guardadas tanto en equipos de cómputo, discos duros o cualquier otro dispositivo donde suele recopilarse parte de la historia de la organización social, con fotos, informes, videos, reportes, expedientes o listado de contactos, a los que se podría acceder de dos formas principalmente: en línea o físicamente, lo que podrían dar paso al robo de datos para usarlos posteriormente o hacerlos desaparecer. Esto da pistas de los cuidados que debe tener dicha información.



DISPOSITIVOS

En cuanto a las herramientas digitales que utilizan en el trabajo de las organizaciones aparecen como fundamentales el teléfono celular y la computadora, como es de prever, y en muchos casos también discos duros externos y cámaras.

La computadora, por tanto, es clave para trabajar la seguridad digital. Casi todas las organizaciones participantes en el diagnóstico tienen computadoras de escritorio, con sistema operativo Windows (salvo una que usa Linux en dichas máquinas). Esto es un primer factor de riesgo, porque se sabe que el *software* de Microsoft (Crespo, 2016) posibilita 'fuga' de información, tanto por fallas como por política de la empresa. Por ejemplo, se han encontrado habitualmente las llamadas 'puertas traseras', que conectan con los servidores de la corporación sin que el o la usuaria lo sepa; también ha sido comprobado que Microsoft ha colaborado con agencias de seguridad (como la NSA) para proporcionar los datos de miles de personas (Tubella, 2013); además de los virus, *malware* y *spyware* a los que son susceptibles de infectarse los programas que corren bajo este sistema operativo.

La computadora, es clave para trabajar la seguridad digital. Casi todas las organizaciones participantes en el diagnóstico tienen computadoras de escritorio, con sistema operativo Windows

El uso de antivirus no es tan generalizado como pensábamos (o no están debidamente actualizados), y tampoco el de contraseñas complejas tanto para dispositivos como para las plataformas utilizadas.

El recomendable uso de discos duros externos para tener respaldos de las informaciones es muy habitual en las organizaciones. Pero faltaría tener una política de respaldos clara y realista, que propicie un autocuidado convenientemente

Más importancia aún está cobrando el teléfono celular, que es un aparato inseguro en sí mismo: solemos llevarlo encima, por lo que van conectándose a distintas antenas o redes, y es fácil de perder o que nos lo roben; en los de última generación (o smarthphone) guardamos por comodidad una gran cantidad de información, además de que con ellos podemos estar en distintas plataformas de comunicación; los sistemas operativos predominantes son poco adaptables a las necesidades particulares de cada quien y muchas veces debemos confiar a ciegas en las aplicaciones que instalamos (y otras no podemos desinstalarlas). Todo ello hace que sean ventanas al mundo, por las que nos informamos y comunicamos, pero también por donde se escapan datos importantes sin que lo sepamos.

El recomendable uso de discos duros externos para tener respaldos de las informaciones es muy habitual en las organizaciones. Pero faltaría tener una política de respaldos clara y realista, que propicie ese autocuidado convenientemente. Al igual que nos encontramos que se usa el usb como lugar de almacenamiento, pero es un dispositivo muy vulnerable.

SOFTWARE

En cuanto a las aplicaciones y programas que se usan, además del sistema operativo mencionado, vemos el uso constante de las redes sociales comerciales, sobre todo Facebook; las videollamadas por Skype (propiedad de Microsoft); el almacenamiento en la nube (con Dropbox o Google

Drive); el uso del correo electrónico con Gmail; todo ello poco recomendable, por ser herramientas que no son libres, por lo tanto no hay forma de auditarlas, y pertenecientes a corporaciones 'amigas' de las autoridades. Igual pasaría con el mencionado WhatsApp. Todas ellas, además, susceptibles de contagiar virus o de ser vulneradas, al ser las más comerciales.

En los talleres de diagnóstico hubo interés por saber más acerca de qué es el **malware**, y conocer qué son los metadatos que también afectan a la seguridad.

ACTORES

Existe mucha coincidencia entre las organizaciones sobre qué actores pueden estar interesados en la información sensible que manejan, y qué podrían conseguir.

Se mencionaron instancias de Gobierno Federal, principalmente Procuraduría General de la República (PGR), Policía Federal y Centro de Investigación y Seguridad Nacional (CISEN); de Gobierno de Chiapas, como Policía Estatal y algunas secretarías; de Gobiernos locales, con la policía a su servicio; de grupos de choque o parapoliciales, que suelen ser tolerados (cuando no impulsados y soportados) por instancias de gobierno; grupos del crimen organizado o narcotráfico; y empresas extractivistas con intereses en la zona, como mineras, extractoras de agua, monocultivos, turísticas, etc. También destaca la mención en varios casos de los servicios de inteligencia, tanto de México

En los talleres de diagnóstico hubo interés por saber más acerca de qué es el malware, y conocer qué son los metadatos que también afectan a la seguridad

Se reconocen espías en las actividades o intentos de infiltración en reuniones. Hay casos de desaparición de documentos en las computadoras y de vigilancia in situ cuando van a realizar actividades

con el comentado CISEN, como otras: CIA (Estados Unidos) y Mossad (Israel), que tienen medios y recursos para hacerse con la información que manejan, como la posibilidad de buscar la cooperación con las empresas dueñas de las plataformas digitales que se usan.

Después, en cada caso particular se comentan actores locales que se encuentran en el territorio donde se desarrolla el trabajo, destacando que en las organizaciones de mujeres estos actores locales son la principal amenaza.

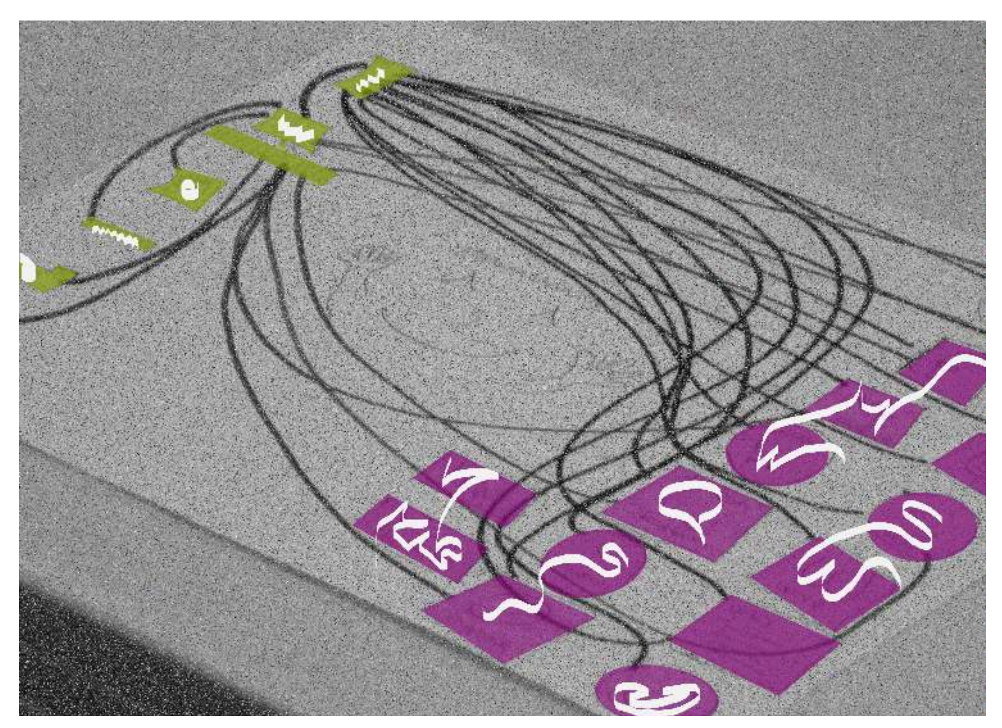
También refieren, en algunos comentarios, que muchas veces estos actores están coordinados o coludidos, "policía y crimen organizado a veces es lo mismo" o que por omisión en la protección de derechos los distintos niveles de gobierno se convierten en parte del problema.

INCIDENTES

Hay que destacar los incidentes de seguridad que nos han compartido algunas organizaciones, que en muchos casos tiene que ver con la información. Por ejemplo, es habitual que el teléfono de la oficina y los personales tengan ruidos e interferencias, que hayan tenido amenazas por mensajes o vía telefónica, y se mencionan allanamientos en algunas instalaciones. También se reconocen espías en las actividades o intentos de infiltración en reuniones. Hay casos de desaparición de documentos en las computadoras y de vigilancia *in situ* cuando van a realizar actividades.

Otra situación que se está haciendo cada vez más común en Chiapas con organizaciones sociales, y también con los grupos de base que acompañan, es la difamación en redes sociales, sobre todo Facebook y cadenas de WhatsApp, que están vulnerando la seguridad de las personas defensoras.

Para cerrar el capítulo de hallazgos encontrados en la investigación, queremos hacernos eco de comentarios que surgieron en distintas ocasiones referidos a la necesidad de que sus propias financiadoras comiencen a mirar el tema de la seguridad digital para poder tener comunicaciones más seguras con ellas y de este modo cuidar las informaciones de los procesos apoyados en cada momento en el que esta información de comparte y almacena. Reivindican que "la seguridad digital, así como la integral, es algo colectivo".



Los desafíos continúan siendo muchos y lograr sensibilizar a quienes aún no miran el tema de la seguridad en las comunicaciones es el primer paso

Hemos encontrado personas con ganas de aprender nuevas herramientas y adquirir prácticas que reduzca los riesgos en el trabajo de las organizaciones, si bien es cierto que siempre hay disparidad en el conocimiento sobre estos temas, la intención es hacer el esfuerzo y apoyarnos entre todas y todos, para caminar en esa dirección.

“Algún acuerdo de seguridad implica que muchísima gente esté en la misma sintonía y eso es bien complicado. Si de por sí es complicado hacerlo al interior del grupo, incluso para comunicarnos por Telegram y no Whatsapp, o luego querer bajar el Signal a muchos les da flojera, o no le entiende o no cabe en el móvil, bueno pues entonces acabas usando la misma chingadera de siempre.”

2.3 Los retos y necesidades

En el camino de esta investigación nos hemos encontrado con grandes desafíos. Sobre todo hemos ratificado en voz de las personas participantes los **cómos** y los **porqués** de la necesidad de mirar la “seguridad digital” desde dentro de las organizaciones. Si bien es cierto que en este proceso de diagnóstico participativo hemos hallado preocupación por el tema de la seguridad digital entre las organizaciones con las que hemos trabajado, los desafíos continúan siendo muchos y lograr sensibilizar a quienes aún no miran el tema de la seguridad en las comunicaciones es el primer paso.

En sí mismo, hacer un verdadero proceso de ‘apropiación’ a largo plazo es un reto. A eso podemos

sumar que, desde los grupos y organizaciones que pretendemos acompañar dichos procesos, aún no tenemos suficientes ejercicios 'de largo plazo' realizados ni contamos con herramientas adecuadas que nos puedan apoyar a 'medir' los resultados. Generar estas herramientas es, en sí misma, una tarea a desarrollar.

Jorge Hernández, del **Frayba**, una organización que ya ha transitado estos caminos de la apropiación, nos comentaba que "ha sido un proceso de poco a poco, de unos ocho años, y para esto ha sido básico buscar alianzas con otro colectivos que quieran apoyar". Además nos hablaba de la importancia de herramientas de formación, como Moodle, que queda **online** para revisar cuando se necesite, sirve para documentar los aprendizajes y sistematizar el proceso.

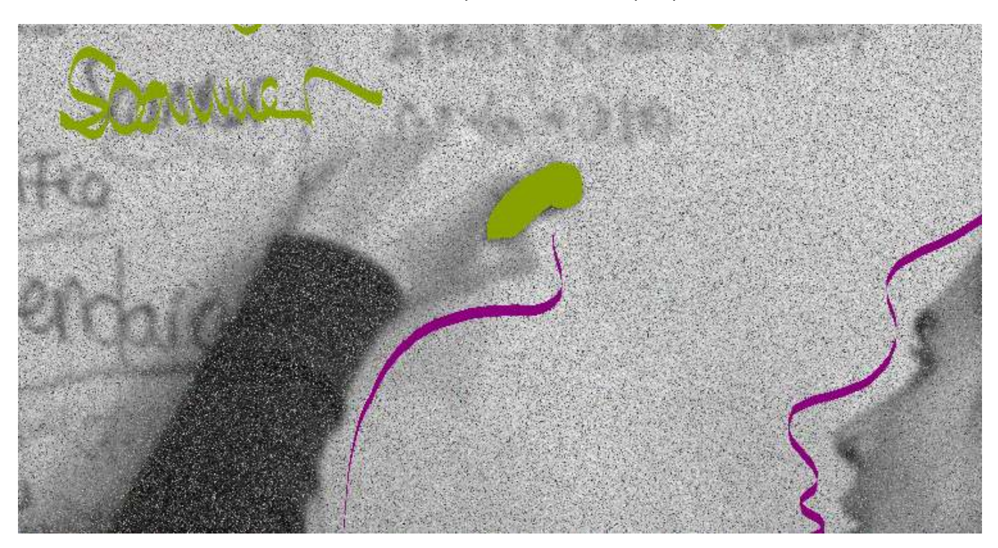
Resulta importante comprender que el uso de guías, manuales o plataformas de aprendizaje serán necesarias en la medida que respondan estrictamente a las acciones y herramientas que se visualizan y aprenden durante los talleres, y no como supletorios de éstos. En ese sentido, tener la capacidad de proporcionar acompañamiento 'suficiente' para reducir los momentos de 'angustia' o frustración durante el proceso de aprendizaje es indispensable.

Los grupos y organizaciones que realizan acompañamientos a otros y otras en diversos temas saben de sobra la importancia de hacerlo de forma procesual. En el marco de adopción de nuevas tecnologías para la autodefensa digital esta característica presenta además desafíos propios.

Aún no tenemos suficientes ejercicios 'de largo plazo' realizados ni contamos con herramientas adecuadas que nos puedan apoyar a 'medir' resultados. Generar estas herramientas es, en sí misma, una tarea a desarrollar

Primero, nos encontramos con el hecho de incorporar la 'seguridad digital' como una parte más de las acciones de 'seguridad integral'. No en pocas ocasiones, las intrusiones a las informaciones y conversaciones que manejan activistas y defensores de derechos humanos continúan viéndose como algo que pudiera suceder a otras y otros, pero no a ellas y ellos mismos.

Además nos encontramos con grupos que en su labor cotidiana poseen una gran carga de actividades. En ese sentido resultará necesario aprender a gestionar el tiempo respecto a los flujos de trabajo actual y los tiempos dedicados a las tareas de mejorar su seguridad digital, para que resulten verdaderamente útiles a largo plazo. También hemos constatado que está instalado un cierto temor al aprendizaje de nuevas tecnologías. Las resistencias a 'lo nuevo' son muy comunes, pero el hecho de que la tecnología continúe bajo el velo de ser una 'cosa de expertos' ralentizaría aún más los procesos de apropiación.



Si a eso le sumamos el creciente uso de dispositivos móviles y la contradictoria sensación de 'desprotección' y 'necesidad' que las personas defensoras manifiestan en su uso, el tema cobra dimensiones más complejas.

Una participante nos compartía una reflexión al respecto: "sería importante un acompañamiento con plazos claros y que empiece con cosas muy sencillas pero que llevan tiempo, sería bueno darnos plazos para que nos demos cuenta que eso tiene que estar dentro de nuestra planeación, ser tomado en serio por el equipo".

Así, en este hilo de retos a considerar es importante destacar la necesidad de generar acuerdos colectivos al interior de cada una de las organizaciones, acuerdos surgidos de ellas y ellos en relación a las prácticas que reconocen como 'inseguras' y de la información sensible que manejan pero también en relación a la disposición al cambio y aprendizajes que ello implique. Estos acuerdos deben ser firmes y progresivos y exigen un nivel de compromiso tanto desde el acompañamiento como de las personas acompañadas.

En este paso, privilegiamos resoluciones 'simples' pero que en el día a día llevan cambios de hábitos arraigados y que además deben ser adoptados por cada una de las personas integrantes de los equipos. Así, vemos cómo la relación persona-dispositivo necesita una atención de una-a-una, uno-a-uno y hacerlo de este modo implica tiempos y esfuerzos adaptados. Ganar confianza con el uso de las tecnologías es importante a la hora de po-

La relación persona-dispositivo necesita una atención de una-a-una, uno-a-uno y hacerlo de este modo implica tiempos y esfuerzos adaptados

Desmitificar el hecho aún vigente de que "usar tecnologías libres es más seguro, pero es más difícil"

der generar cambios a largo plazo y eso requiere pasar por el mismo lugar una y otra vez.

"Hay cosas que serán a corto, mediano y largo plazo. Algunas que precisamente son hábitos que no los hacemos y no lo vemos necesario porque estamos en esa costumbre de que no lo ponemos ahí en tela de juicio sino hasta que algo pase", nos decía otra persona participante.

Desde los grupos que decidimos adoptar las prácticas de educación popular solemos decir que iremos al 'paso del más lento'. Este es un acuerdo que establecemos junto a las personas acompañadas en el cual todas y todos estamos conscientes. Sin embargo, en la práctica, hacerlo realidad implica un compromiso de atención, paciencia y compartición que aún estamos aprendiendo.

De este modo, romper el 'estigma' que rodea las dificultades de mejorar prácticas digitales y el uso de sistemas operativos y/o programas libres es otro de los grandes desafíos. Consideramos que para hacerlos realidad, necesitamos además que 'pase por el cuerpo', es decir que cada quien pueda aprender desde sus propias experiencias de uso y no únicamente mirando los fallos y errores como situaciones que se pueden resolver desde el 'servicio técnico', sino también como acciones en las cuales puedo contar con mi compañero o compañera de equipo para poder preguntar, gestionar, resolver. Y claro, desmitificar el hecho aún vigente de que "usar tecnologías libres es más seguro, pero es más difícil".

Como mencionábamos en el apartado anterior, los niveles de conocimientos respecto a las tecnologías entre las propias organizaciones es muy dispar. Para algunas este era su primer acercamiento al tema de la seguridad digital por lo que las tareas a implementar en estos casos distan considerablemente de quienes ya han tenido talleres eventuales respecto al tema.

Por otro lado el mayor desafío se presenta al interior de las propias organizaciones las cuales suelen tener conocimientos muy diferentes sobre este tema. Como hallazgo importante vimos que las organizaciones no tienen personas encargadas específicamente del tema informático y muchas veces ni siquiera alguien externo, pero de confianza, que se encargue de revisar sus equipos tecnológicos.

En general, aunque han resultado de cierta ayuda, los talleres de seguridad digital a los que son invitadas reúnen a pocas personas de diferentes organizaciones y condensan gran cantidad de herramientas a aprender en poco tiempo. Es tan sólo 'una probadita', y según lo experimentado por las propias personas participantes, este modelo no ha logrado afianzar prácticas ni transmisión de dichos conocimientos hacia las demás personas de las organizaciones y lo aprendido se queda en las personas asistentes, sin posibilidad de poder hacer uso cotidiano de ellas.

Las organizaciones no tienen personas encargadas específicamente del tema informático y muchas veces ni siquiera alguien externo, pero de confianza, que se encargue de revisar sus equipos tecnológicos

Respecto al acompañamiento necesario, nos mencionaban que "sea práctico, que sea sencillo y empezar de poquito a más". Y otras añadían: "Eso

Algunas participantes aludían con entusiasmo a la posibilidad de hacer transición al software libre: "No he usado ni conozco mucho, pero creo que también es una opción que concuerda mucho con el discurso que tenemos"

de las capacitaciones express no me agradan porque somos muy lentas y además creo que no se entiende todo muy bien (...) Irnos paso a paso. Quizás en una primera implementación poner en práctica algunas cosas que son más sencillas, y ver cómo las caminamos y luego seguimos con otras. Con una secuencia, no de tajo". Además de que incluían en la reflexión la importancia de la evaluación de cada paso en el proceso, porque hasta ahora los talleres eventuales que han tenido, no contaron con algún tipo de seguimiento posterior.

En este sentido, la capacitación interna para poner en común todas las prácticas y herramientas es fundamental y los primeros esfuerzos están puestos en acordar acciones mínimas para la seguridad digital que podamos implementar para todas las personas de los equipos.

Sucede también que no todas las personas al interior de las organizaciones manejan información sensible que requiera cuidados más atentos y/o que dicha información esté centralizada en una o pocas personas. Para estos casos, es imprescindible readaptar los procesos de aprendizaje en relación a lo que cada área de trabajo de las organizaciones necesita y generar políticas de transmisión y resguardo de la información que permita poner a disposición dicha información de maneras más cuidadosas.

Por último, es interesante mencionar que algunas participantes aludían con entusiasmo a la posibilidad de hacer transición al software libre: "No he usado ni conozco mucho, pero creo que también es

una opción que concuerda mucho con el discurso que tenemos, que al final de cuentas es un discurso de una organización no gubernamental en la que vamos contra algunas cuestiones, entonces eso se me hace algo muy chido, el poder concordar el discurso con las acciones".

A lo que también hacía referencia Jorge Hernández cuando nos compartía el proceso en el Frayba, "por una congruencia política, es decir, si somos una institución que le apostamos a ser antisistémicos y le estamos pagando al hombre más rico y no tenemos el control de los programas que estamos utilizando, entonces fue así que decidimos este proceso de cambio a software libre".



3. Conclusiones



México, como hemos referenciado en el apartado de contexto de este informe, ha vivido varios casos documentados de vigilancia hacia defensoras y defensores de derechos humanos, periodistas y activistas.

Nos resultó muy enriquecedor compartir este camino de aprendizajes mutuos, que en algunos casos seguirá mediante un acompañamiento más personalizado

Éste sería motivo suficiente para emprender un proceso de diagnóstico de seguridad digital en organizaciones sociales de Chiapas, sumado al tratamiento que tienen nuestros datos por parte de las plataformas digitales, con la consecuente violación de la privacidad y otros derechos. En la actualidad, todo ello es conocido por la sociedad civil organizada, de ahí la necesidad de revisarse y atender al tema, porque es preferible 'prevenir que lamentar', adelantarse a cualquier circunstancia y tener algunos conocimientos y herramientas que nos ayuden en nuestra seguridad. También la digital.

Para esta investigación trabajamos con ocho organizaciones, de reconocida trayectoria en Chiapas, partiendo de una metodología participativa. Nos resultó muy enriquecedor compartir este camino de aprendizajes mutuos, que en algunos casos seguirá mediante un acompañamiento más personalizado.

Hemos constatado que la seguridad integral forma parte del trabajo de estas organizaciones. En el trabajo que realizan muchas veces corren peligro, con el fin de que se respeten derechos fundamentales. Actores que entorpecen y que violan estos derechos hay varios, que conocen bien. De ahí que quieran que se sumen los autocuidados digitales

también a sus prácticas. Es más, se hace necesario poner énfasis en la discusión política de la seguridad digital para tomarla como práctica colectiva de la sociedad civil.

Como decíamos hace unos meses respecto a esto mismo:

"Nos interesa hacerlo desde la perspectiva de los derechos colectivos y en ese sentido las personas con las que trabajamos esperan de nosotras y nosotros que además de apoyarles a resolver problemas técnicos, entendamos los problemas de sus luchas, que podamos hablar otros lenguajes que les sean cercanos; es más, necesitamos crear lenguajes que nos sean comunes [porque no, no están inventados: entre el lenguaje de las y los defensores de 'primera línea' y las y los defensores de los territorios de Internet hay aún muchos abismos que cruzar]... Probemos la perspectiva de autodefensa y soberanía tecnológica desde la construcción colectiva de las respuestas que necesitamos. Las personas que nos llaman buscando soluciones a sus problemas de vigilancia, acoso o intimidación esperan de nosotras y nosotros que podamos acompañarlas [también] con cariño" (Sursiendo, 2018).

Se hace necesario poner énfasis en la discusión política de la seguridad digital para tomarla como práctica colectiva de la sociedad civil.

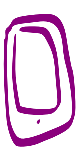
Este diagnóstico es un paso más para tomar conciencia de los riesgos, de los actores involucrados, de las prácticas que tenemos, de las herramientas digitales que utilizamos. La adopción de nuevas rutinas y de nuevo software es un proceso que no puede ser inmediato. La diferencia está en las formas en las que transitamos

esos procesos de uso y apropiación: “apenas inicia el acercamiento a la idea de que para trabajar tecnologías desde una perspectiva social necesitamos ir allí donde las personas están. Habitando esos espacios podremos romper con la idea de que la ‘inclusión’ es ‘traer’ a las personas a nuestras formas de ver y hacer tecnología para pasar a comprender que la inclusión tiene que ser multidireccional” (Sursiendo, 2018).

Seguiremos en la defensa de los derechos digitales colectivos, en la disputa por el territorio Internet, para que sea más abierto, libre, inclusivo y biodiverso

Desde las organizaciones sociales nos piden acompañamiento más enfocado, con más tiempo, yendo poco a poco, desde lo básico. Quienes nos dedicamos a estos temas debemos hacer ese acompañamiento de forma procesual, lento, constante, para todas las personas de la organización, adecuado a las necesidades, con materiales de apoyo, y pidiendo el compromiso de las organizaciones involucradas, generando acuerdos firmes y de largo plazo. Ha sido y está siendo un gran aprendizaje, pero también un enorme desafío.

Seguiremos en la defensa de los derechos digitales colectivos, en la disputa por el territorio Internet, para que sea más abierto, libre, inclusivo y biodiverso. Salud.



4. Referencias



Ahmed, Azam y Perlroth, Nicole (2017) 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. New York Times.
https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Aristegui Noticias (2012) Gobierno federal vía Sedena compró 5 mil mdp en equipo para espionaje, 16 de Julio de 2012.
https://aristeguinoticias.com/1607/mexico/gobierno-federal-via-sedena-compro-5-mil-mdp-en-equipo-para-espionaje/

Bauman, Zygmunt y Lyon, David (2013) Vigilancia líquida. Paidós

CNNMéxico (2014) 20 puntos clave en las nuevas leyes sobre Telecomunicaciones. Revista Expansión, 9 de julio de 2014.
https://expansion.mx/nacional/2014/07/09/20-puntos-clave-en-las-nuevas-leyes-sobre-telecomunicaciones

Crespo, Adrián (2016) Snowden se muestra atemorizado de las puertas traseras existentes en los productos de Microsoft (23 marzo, 2016)
https://www.redeszone.net/2016/03/23/snowden-se-muestra-atemorizado-las-puertas-traseras-exitentes-los-productos-microsoft/

Desjardins, Jeff (2018) What Happens in an Internet Minute in 2018?
http://www.visualcapitalist.com/internet-minute-2018/
Escobar, Arturo. 2010. Territorios de diferencia. Lugar movimientos vida redes. Envión Ediciones.

Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. Informe.

https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

Internet World Stats (2018) Internet Usage and Population. https://www.internetworldstats.com/stats12.htm

Lacort, Javier (2015) México es el país que más gastó en Hacking Team para espiar a sus ciudadanos. Hipertextual, Jul 7, 2015
https://hipertextual.com/2015/07/hacking-team-mexico

Laurant, Cédric y Laguna Osorio, Monserrat (2014) El caso FinFisher. Reporte Mexico de la organización SonTusDatos para Global Information Society Watch.
https://www.giswatch.org/hu/node/4955

Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) (2014)
http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_150618.pdf

Mariscal, Ángeles (2013) Gumalo, activista de las redes sociales, enfrentará juicio en libertad. En Chiapas Paralelo.
https://www.chiapasparalelo.com/noticias/chiapas/2013/11/gumalo-activista-de-las-redes-sociales-enfrentara-juicio-en-libertad/

Miguel, Pedro y Molina, Tania (2013) Empresas de espionaje cibernético buscan ampliar mercado en México. Periódico La Jornada, 5 de septiembre de 2013, p. 4.
https://www.jornada.unam.mx/2013/09/05/politica/004n1pol

Pérez de Acha, Gisela (2016) El Foro de Gobernanza de Internet en un país autoritario (08 de diciembre, 2016)

https://www.derechosdigitales.org/10695/el-foro-de-gobernanza-de-internet-en-un-pais-autoritario/

Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la vigilancia fuera de control.
https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.
https://r3d.mx/2017/06/19/gobierno-espia/

Reforma (2013) Derrocha la PGR en equipo espía. 06-Jul-2013
https://hemerotecalibre.reforma.com/20130706/interactiva/RNAC20130706-005.JPG&text=Hacking+Team&tit=Derrocha%20la%20PGR%20en%20equipo%20esp%EDa

Robles Maloof, Jesús (2013) 90 días. Gustavo, libre. Revista electrónica Sin Embargo (noviembre 12, 2013)
https://www.sinembargo.mx/12-11-2013/3018980
Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso.
https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

SIPAZ (2010) Chiapas: Denuncia de persecuciones a periodistas.
https://sipaz.wordpress.com/2010/11/17/chiapas-periodista-teme-por-su-integridad/

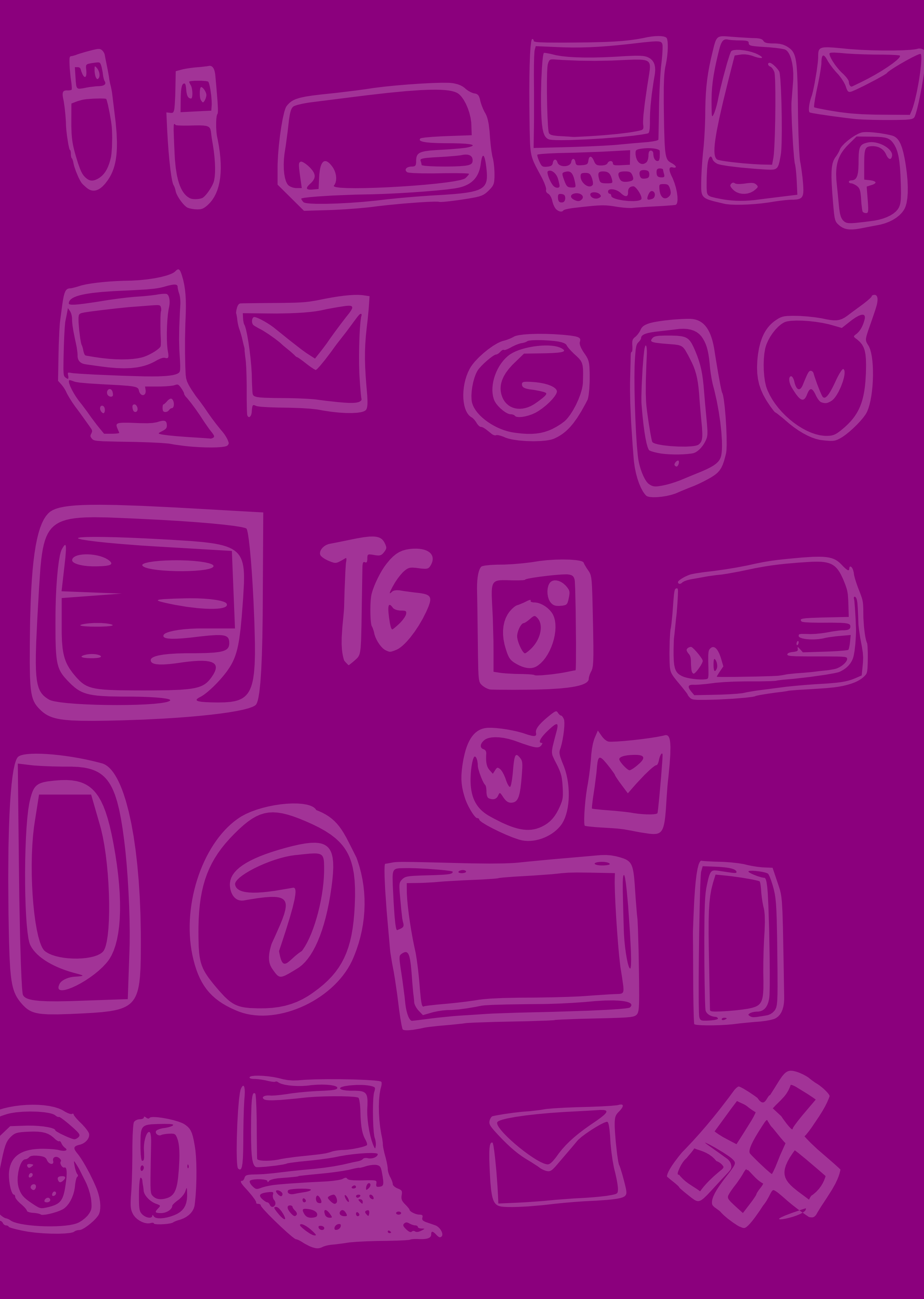
Sparrow, Elijah (2014) Vigilancia digital. Reporte de LEAP Encryption Access Project.
https://giswatch.org/es/thematic-report/communications-surveillance/vigilancia-digital

Sursiendo (2018) ¿Por qué pensar en soluciones 'low-tech'? Blog Sursiendo (mayo de 2018).
https://sursiendo.com/blog/2018/05/por-que-pensar-en-soluciones-low-tech/

Tubella, Patricia (2013) La NSA pagó millones a los gigantes de Internet por colaborar en el espionaje. El País, 23 de agosto de 2013.
https://elpais.com/internacional/2013/08/23/actualidad/1377272049_738995.html

Wikileaks (2015) Hacking Team. Resultados de la búsqueda 'Chiapas'.
https://wikileaks.org/hackingteam/emails/?q=chiapas&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult

Wikipedia (s/f) Investigación-Acción participativa
https://es.wikipedia.org/wiki/Investigaci%C3%B3n-Acci%C3%B3n_participativa


TG

Este informe se realizó y diseñó con software libre: LibreOffice, Inkscape, Gimp, Scribus y Krita. Se usaron las fuentes tipográficas libres "Abel" en 12 puntos para el cuerpo del texto y "Gloria Hallelujah" en 14 puntos para los títulos.

Este informe se imprimió en La Cosecha, enero de 2019.
San Cristóbal de Las Casas, Chiapas, México.


Iurviendo
Comunicación
Cultura Digital